

FILED

MAY 10 2024

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
Information Associated with Kik Usernames
'kissmeboopl_3z8' That is Stored at a Premises Controlled by
MediaLab.ai, Inc.

Case No.

24-mj-340-CDL

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 2252(a)(2) and (b)(1)
18 U.S.C. §§ 2252(a)(4)(B) and
(b)(2)

Offense Description
Receipt and Distribution of Child Pornography
Possession of and Access with Intent to View Child Pornography

The application is based on these facts:

See Affidavit of SA Thomas Oelschlager, FBI, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Thomas Oelschlager, FBI

Printed name and title

Subscribed and sworn to by phone.

Date: May 10, 2024City and state: Tulsa, Oklahoma

Judge's signature

Christine D. Little, U.S. Magistrate Judge

Printed name and title

Affidavit in Support of an Application for a Search Warrant

I, Thomas Oelschlager, being duly sworn, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with Kik username “**kissmeboopl_3z8**” that is stored at premises owned, maintained, controlled, or operated by MediaLab.ai, Inc., a holding company of consumer internet brands, offering messaging applications, online education platform, and various applications for users headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab.ai, Inc. to disclose to the government records and other information in its possession, pertaining to the individuals associated with Kik username “**kissmeboopl_3z8**” (hereinafter the “**SUBJECT ACCOUNT**”).

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Special Agent with the FBI and have been since September 2018. I am currently assigned to the Oklahoma City Division. As a Special Agent, my duties include investigating violations of federal

criminal law and threats to national security. In addition to formalized training, I have received extensive training through my involvement in numerous investigations working alongside experienced law enforcement officers at both the federal and local level. My investigations include, but are not limited to crimes against children, complex financial crime, and Indian Country violations. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) have been committed by the individuals associated with the **SUBJECT ACCOUNT**. There is also probable cause to search the information described in Attachment A for

evidence of this crime and contraband or fruits of this crime as described in Attachment B.

Jurisdiction

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

Background of NCMEC and the CyberTipline Program

6. The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further the mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Program. NCMEC makes information submitted to the CyberTipline and Child Victim Identification Program available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers (ESPs), law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC performs its programs of work pursuant to its own private mission and independent business operations. NCMEC does not act in the

capacity of or under the direction or control of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties,

7. NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and ESPs can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sex abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. CyberTipline Reports (CyberTips) are distributed by NCMEC analysts to law enforcement agencies who may have legal jurisdiction in the place that victims and suspects are believed to be located based on information provided in the CyberTips.

Probable Cause

8. On March 29, 2024, Kik submitted a CyberTip to the National Center for Missing and Exploited Children (NCMEC) regarding Kik user **kissmeboopl_3z8** sending child pornography to other Kik users. Kik provided NCMEC three videos which were sent by Kik user **kissmeboopl_3z8** as described below:

9. On January 29, 2024, at 13:05 UTC, Kik user **kissmeboopl_3z8**, using IP address 104.156.29.62, transmitted file 41b4e709-458f-423c-aaef-8e89e0b38869.mp4 to another Kik user via private message. This file is a video which depicts a white pubescent minor female with light brown hair being penetrated vaginally by a white

adult male. The female was wearing a light-colored top and had green underwear pushed down to her legs.

10. On January 26, 2024, at 22:00 UTC, Kik user **kissmeboopl_3z8**, using IP address 104.156.29.62, transmitted file bdd2e447-bb16-4d34-b833-b9599b0f553b.mp4 to another Kik user via private message. This file is a video which depicts a white prepubescent female with blonde hair being digitally penetrated. The female was wearing a blue and green bikini top but was nude below.

11. On January 26, 2024 at 22:00 UTC, Kik user **kissmeboopl_3z8**, using IP address 104.156.29.62, transmitted file 543d6367-1b78-4426-b17b-4854693bfla0.mp4 to another Kik user via private message. This file is a video which depicts a white prepubescent male holding up his light-colored shirt with grey underwear was pushed down to his legs. A white adult blonde female was performing oral sex on the prepubescent male.

12. On April 24, 2024, FBI Tulsa received a lead from FBI St. Louis Division regarding Kik user **kissmeboopl_3z8**. FBI St. Louis is investigating Kik user **Jayjay87888990_0kw** which involved the sexual exploitation of children. As part of the investigation, a search warrant was submitted to Kik for the contents of Kik user **Jayjay87888990_0kw**'s account. The information returned from Kik included conversations Kik user **Jayjay87888990_0kw** had with other Kik users discussing the sexual abuse of children. One of these users were identified as Kik user **kissmeboopl_3z8**. The information provided by Kik shows the content of messages sent by Kik User **Jayjay87888990_0kw** and the recipient but does not show messages received by Kik User **Jayjay87888990_0kw** from other users.

13. A sampling of the messages sent from Kik user **jayjay87888990_0kw** to Kik user **kissmeboopl_3z8** indicate that the two users are discussing sexually abusing children. The responses that **jayjay87888990_0kw** gave **kissmeboopl_3z8** indicate that **kissmeboopl_3z8** had been talking about sexually abusing children. The messages are shown below:

Sender_id	Recever_id	Message	Sent at
jayjay87888990_0kw	kissmeboopl_3z8	You got that pussy yet	2023-11- 16T03:36:24Z
jayjay87888990_0kw	kissmeboopl_3z8	How old was she when you got her	2023-11- 16T03:37:08Z
jayjay87888990_0kw	kissmeboopl_3z8	Indiana	2023-11- 16T03:38:49Z
jayjay87888990_0kw	kissmeboopl_3z8	Yes I've got her	2023-11- 16T03:39:00Z
jayjay87888990_0kw	kissmeboopl_3z8	You got that pussy yet	2023-11- 16T03:39:39Z

14. Open source research identified Salina-Spavinaw Telephone Company as the service provider of IP address 104.156.29.62. On April 23, 2024, the FBI received a response to an administrative subpoena served to Salina-Spavinaw Telephone Company regarding IP address 104.156.29.62 as listed below:

Subscriber Name: Arthur and Connie Cason

Subscriber Address: 46 Spring Cove Ln., Salina, OK 74365

Subscriber Cell Phone: 918-770-6081 and 918-530-5858

Email Address: cd_cason@yahoo.com

15. The address of 46 Spring Cove Ln., Salina, Oklahoma is within the Northern District of Oklahoma.

16. On April 29, 2024, U.S. Magistrate Judge Mark T. Steele approved a search warrant for the premise of 46 Spring Cove Ln. in Salina, Oklahoma in case number 24-MJ-310-MTS. The warrant is set to be executed on May 13, 2024.

Background on Kik and MediaLab.ai, Inc.

17. Kik is owned and operated by MediaLab.ai, Inc., a holding company of consumer internet brands, offering messaging applications, online education platform, and various applications for users headquartered in Santa Monica, California. Kik advertises itself as “the first smartphone messenger with a built-in browser.” Kik Messenger allows users to “talk to your friends and browse and share any web site with your friends on Kik.” According to their website, Kik Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat

experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control of with whom they communicate. In addition, Kik users can exchange images, videos, sketches, stickers and even more with mobile web pages.

18. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads and is available on the Google PlayStore for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

19. In general, providers like Kik ask their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address. However, Kik does not verify that information. Kik also retains certain transactional information about the creation and use of each account on their systems, including the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account.

20. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

21. Given the ability for users to create multiple accounts that are not linked to a specific mobile device (i.e. a phone number), it has become a popular app used by people involved in the collection, receipt, and distribution of child pornography.

22. In my training and experience, an application user's IP log, stored electronic communications, and other data retained by the provider, can indicate who has used or controlled the application account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Kik account at a relevant time. Further, Kik account activity can show how and when the account was accessed or used. For example, as described herein, Kik logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Kik access, use, and events relating to the crime under investigation. Additionally, Kik account activity may provide relevant insight into the Kik account owner's state of mind as it relates to the offense under investigation. For example, information on the Kik account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal

evidence from law enforcement).

23. Therefore, the computers and systems of Kik, owned and operated by MediaLab.ai, Inc., are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Kik, such as account access information, transaction information, and other account information.

Characteristics Common to Individuals Who Exhibit a Sexual Interest in Children

24. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who exhibit a sexual interest in children, and who distribute, receive, possess, and/or access with intent to view child pornography:

1. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;
- li. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;
- lii. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos,

photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

- liii. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, on their person, to enable the individual to view the child pornography images, which are valued highly. Such individuals do not like to be away from their child pornography images for an extended period of time. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;
- liv. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;
- lv. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared; and

- lvi. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

Information to be Searched and Things to be Seized

25. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab.ai, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

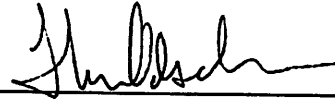
Conclusion

26. Based upon the facts set forth in this affidavit, I believe that there is probable cause to believe that the location described in Attachment A contains evidence of violations of Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography).

27. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on MediaLab.ai, Inc. Because the warrant will be served on

MediaLab.ai, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Thomas Oelschlager
Special Agent, FBI

Subscribed and sworn by phone this 10th day of May, 2024



CHRISTINE D. LITTLE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the account associated with Kik username “kissmeboopl_3z8” (SUBJECT ACCOUNT), that are stored at premises owned, maintained, controlled, or operated by MediaLab.ai, Inc., a company headquartered at 1222 6th Street, Santa Monica, CA 90401.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MediaLab.ai, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab.ai, Inc., regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab.ai, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab.ai, Inc. is required to disclose the following information to the government for each account listed in Attachment A between November 16, 2023, through February 29, 2024:

- (a) All contact and personal identifying information;
- (b) All activity logs for the account and all other documents showing the user's posts and other Kik activities;
- (c) All photos and videos uploaded by the SUBJECT ACCOUNT and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Kik usernames; groups and networks of which the

user is a member; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of MediaLab.ai, Inc.’s applications;

- (e) All basic subscriber information,
- (f) All call detail records,
- (g) All detailed message logs,
- (h) All content, including but not limited to message content,
- (i) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that account, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (j) All other records and contents of communications and messages made or received by the user, including all Messenger activity, messages, chat history, video and voice calling history, and pending “Friend” requests;
- (k) All “check ins” and other location information;
- (l) All IP logs, including all records of the IP addresses that logged into the account;
- (m) All past and present lists of friends created by the account;
- (n) All records of Kik searches performed by the account;
- (o) The types of service utilized by the user;

- (p) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (q) All privacy settings and other account settings, including privacy settings for individual Kik posts and activities, and all records showing which Kik users have been blocked by the account;
- (r) All records pertaining to communications between MediaLab.ai, Inc. and any person regarding the user or the user's Kik account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252 for the **SUBJECT ACCOUNT**, listed on Attachment A, including:

- (a) Images of child pornography; files containing images and data of any type relating to the sexual exploitation of minors, and material related to the possession or production thereof, as defined in 18 U.S.C. § 2252;
- (b) Information, correspondence, records, documents, or other materials pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors;
- (c) Communications between the **SUBJECT ACCOUNT** and others pertaining to the receipt, distribution, and/or possession of child pornography from November 16, 2023, through February 29, 2024;

- (d) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- (e) Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and
- (f) The identity of the person(s) who created or used the SUBJECT ACCOUNT, including records that help reveal the whereabouts of such person(s).